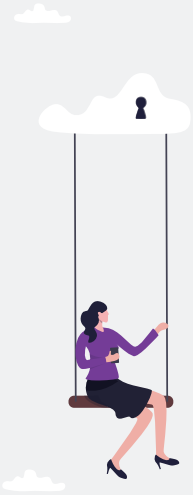
proofpoint.

LIBRO ELECTRÓNICO



Protección para Microsoft 365

Cómo una solución de seguridad especializada puede proteger a sus usuarios, garantizar la seguridad de sus datos e incrementar el valor de su inversión en la nube

Introducción

Pocas herramientas son tan imprescindibles para las empresas actuales como Microsoft 365. En muchos casos, esta plataforma es clave para el teletrabajo, la colaboración global y la nube (y hasta sinónimo de todos estos términos).

Lamentablemente, su ubicuidad y su papel central en el lugar de trabajo lo convierten en un objetivo primordial para los ciberdelincuentes y, a menudo, en el principal vector para comprometer a sus víctimas. Al mismo tiempo, la rápida adopción del teletrabajo y el trabajo híbrido ha colocado las amenazas internas y la pérdida de datos en el punto de mira de la seguridad.

Los ataques avanzados actuales se basan en el phishing y la ingeniería social, no solo en los exploits técnicos. Engañan a los usuarios para que instalen ransomware y otros tipos de malware, faciliten sus credenciales, compartan información sensible e incluso transfieran fondos. Además, los ciberdelincuentes están intensificando estos ataques centrados en las personas y los están haciendo más generalizados, caros y sofisticados que nunca.

Su inversión en Microsoft 365 también pierde valor por las molestias que causan las amenazas, el correo masivo y el spam. El elevado volumen de estos mensajes no deseados no solo afecta a la productividad de los empleados, sino que puede desbordar a unos equipos de seguridad y de TI ya de por sí sobrecargados.

Aunque Microsoft 365 es una herramienta de colaboración indispensable, algunos expertos, como Gartner y Forrester, recomiendan aplicar al correo electrónico, la nube y los datos una seguridad más completa que la nativa de la plataforma[1,2].

Este libro electrónico analiza estas amenazas modernas, las mejores prácticas para proteger a los usuarios y los datos, y las funciones que hay que buscar a la hora de ampliar las defensas de Microsoft 365.

1 Mark Harris, Peter Firstbrook, *et al*. (Gartner). "Market Guide for Email Security" (Market Guide para la seguridad del correo electrónico), octubre de 2021.

2 Jess Burn, Joseph Blankenship, *et al*. (Forrester). "Best Practices: Phishing Prevention" (Mejores prácticas: prevención del phishing), noviembre de 2021.

SECCIÓN 1

Cómo atacan los ciberdelincuentes a sus usuarios de Microsoft 365

No sorprende que la mayoría de los ataques dirigidos empiecen en el correo electrónico.

Con técnicas como el phishing o el malware, el correo electrónico permite a los ciberdelincuentes sacar partido con facilidad del factor humano y robar credenciales y datos, entre otros activos. Estas amenazas pueden tener un enorme impacto en las ganancias de la empresa. El coste total medio de una fuga de datos ha alcanzado un récord mundial de 4,35 millones de dólares, lo que supone un impresionante aumento del 43 % en los tres últimos años[3]. En EE. UU., la cifra es incluso mayor, ya que, con un incremento del 15 % frente a 2019, gira en torno a los 9,44 millones[4].

3 Ponemon Institute. "Cost of a Data Breach 2022" y "Cost of a Data Breach 2019" (El coste de una fuga de datos, 2022 y 2019), julio de 2022 y agosto de 2019.

4 *Ibid*.

66 %

de las organizaciones sufrió al menos un ataque de phishing altamente dirigido en 2021

Phishing

En los más de 20 años que hace que los investigadores lo identificaron por primera vez como una amenaza, el phishing se ha convertido en una industria artesanal de todo tipo. Los ciberdelincuentes emplean una amplia variedad de técnicas para robar credenciales, dinero y datos de valor.

El phishing actual es multicapa y consigue sortear muchas de las defensas tradicionales. Los ataques pueden dirigirse a distintos objetivos o bien estar muy focalizados. Muchos emplean malware, pero no todos. Los ciberdelincuentes llegan incluso a enviar mensajes de phishing a través de servicios de marketing legítimos, con el fin de escapar a los filtros de spam y otras medidas de protección.

Cerca del 66 % de las organizaciones sufrió al menos un ataque de phishing altamente dirigido en 2021, mientras que el 65 % sufrió al menos una estafa Business Email Compromise (BEC)[5] (consulte "Estafas BEC y suplantación de identidad de los proveedores" en la página siguiente).

Sea cual sea la táctica utilizada, el éxito de los ataques de phishing es innegable. El año pasado, hasta un 83 % de las organizaciones estadounidenses sufrieron un ataque de phishing que consiguió sus objetivos, frente al 57 % del año anterior[6].

Malware

El AV-TEST Institute registra todos los días más de 450 000 nuevas variedades de malware y aplicaciones peligrosas[7]. Pero la creatividad de los ciberdelincuentes no acaba aquí.

Los atacantes son igual de creativos cuando se trata de buscar nuevos objetivos. Emplean herramientas automatizadas para conseguir información sobre la plantilla de una empresa en sus perfiles públicos de las redes sociales. Saben dónde trabajan los usuarios, saben qué puesto ocupan y conocen sus intereses, sus hobbies, su estado civil, su trayectoria profesional y muchos otros datos.

Esta información sirve a múltiples propósitos, como identificar a los usuarios que poseen los datos o el acceso que buscan, pero también encontrar cebos que resulten suficientemente convincentes en los mensajes de correo electrónico para que los usuarios hagan clic. En cuanto el destinatario muerde el anzuelo, se instala una payload maliciosa en el sistema.

5 Proofpoint. "State of the Phish 2022", febrero de 2022.
6 *Ibid*.
7 AV-TEST Institute. "Malware (https://www.av-test.org/en/statistics/malware/)", consultada en agosto de 2022.

Estafas BEC y suplantación de identidad de los proveedores

Los ataques BEC y la suplantación de identidad de los proveedores se han convertido en una amenaza nueva y peligrosa. Según el FBI, desde 2016 estos ataques han costado a sus víctimas más de 43 000 millones de dólares (en pérdidas reales y potenciales).

En ellos, el atacante se hace pasar por una figura de autoridad, un partner comercial, un cliente o un proveedor. Puede utilizar una dirección de correo electrónico falsificada o un dominio de correo electrónico parecido al real. En algunos casos, emplea una cuenta de correo electrónico legítima pero comprometida, algo casi imposible de detectar únicamente con Microsoft 365. Sea cual sea la táctica, su fin es el mismo: engañar a la víctima para que envíe o desvíe fondos.

Por ejemplo, puede darse el caso de un mensaje de correo electrónico que parece proceder de un proveedor de confianza en el que solicita a un contable que realice operaciones como:

Transferencias de fondos

Desvío de pagos

Cambio de los datos de una cuenta bancaria

En la mayoría de los casos, el dinero va a parar directamente a los bolsillos del impostor. De media, un ataque puede reportarle al atacante casi 180 000 dólares.

Pero los ataques BEC no se limitan a las transferencias bancarias fraudulentas; los ciberdelincuentes pueden engañar a los destinatarios para que les envíen información de identificación personal, datos de nóminas, etc.

Estos ataques se fijan en personas de todos los niveles del escalafón en la empresa, con independencia de su unidad empresarial, departamento o equipo. Por este motivo deberá ampliar la protección contra ataques BEC para hacerla extensiva a todos los miembros de su entorno, en lugar de limitarla a personas específicas.

Compromiso de cuentas

Tener el control de una cuenta de confianza de Microsoft 365 proporciona al ciberdelincuente una enorme cantidad de información que puede usarse como plataforma de lanzamiento de todo tipo de ataques.

Los usuarios con altos privilegios suelen ser blancos habituales. Con acceso a la cuenta de correo electrónico de un CEO o un vicepresidente de RR. HH., el atacante puede acceder a casi cualquier dato de la red. Además, puede sacar provecho de las relaciones de confianza del ejecutivo para lanzar ataques BEC a los partners comerciales. Como consecuencia, no solo se alteran los procesos normales de la organización, sino que puede resultar dañado uno de sus activos más valiosos: su reputación.

Tácticas avanzadas

Casi todos estos ataques utilizan una o varias formas de ingeniería social, el sutil arte de la manipulación. Se trata de persuadir con argucias, de incitar a alguien a hacer algo en contra de su propio interés.

A base de ingeniería social, los atacantes engañan a sus víctimas para que hagan clic en enlaces no seguros, abran adjuntos maliciosos, desvíen dinero y envíen datos confidenciales.

Una de las novedades más inesperadas recientemente ha sido el marcado aumento de los ataques por teléfono. Estos ataques requieren un elevado nivel de interacción directa, ya que los señuelos enviados por correo electrónico no contienen malware ni URL maliciosas. Y, si no se añaden capas de seguridad a Microsoft 365, normalmente pasan desapercibidos. Su objetivo es persuadir a la víctima de llamar a un número falso de atención al cliente.

Una vez que la víctima llama, el atacante le convence de que le brinde acceso remoto a su ordenador o descargue malware manualmente. Nuestros datos muestran que se produjeron más de 100 000 intentos diarios de inicio de ataques telefónicos al día.

SECCIÓN 2

Por qué una seguridad "bastante buena" ya no es suficiente

La seguridad nativa de Microsoft 365 y sus funciones para garantizar el cumplimiento de normativas pueden ser útiles en algunos casos concretos. Pero, a medida que las amenazas se multiplican y evolucionan, pueden hacer falta otras capas de seguridad.

Es posible que, en algunos casos, la ciberseguridad fuera una preocupación menor mientras las organizaciones centraban sus esfuerzos en mantener la viabilidad del teletrabajo y el trabajo híbrido. Ahora que lo peor de la pandemia de COVID-19 ha quedado atrás, muchas empresas desean reforzar su inversión en la nube.

Si las organizaciones no se protegen convenientemente frente a las ciberamenazas y la pérdida de datos, se pueden producir fugas costosas que afecten a su imagen de marca, dañen su reputación y reduzcan sus ganancias. Por eso, ampliar las defensas de Microsoft 365 es esencial para garantizar una seguridad continua y cumplir las normativas en todo momento.

Los ataques actuales tienen como objetivo a las personas

Los ciberdelincuentes saben que la mayoría de las personas de su organización utilizan Microsoft 365 más que ninguna otra herramienta empresarial. Muchos de estos usuarios tienen acceso a fondos o datos de gran valor. Pero otros tienen vulnerabilidades, perfiles de ataque y privilegios de acceso que no son tan evidentes.

Los ciberdelincuentes emplean tácticas de ingeniería social para engañar a los usuarios y conseguir que:

Abran archivos adjuntos infectados

Visiten sitios maliciosos

Proporcionen activos (como credenciales o datos financieros)

Otorguen acceso persistente a sus cuentas a través de OAuth

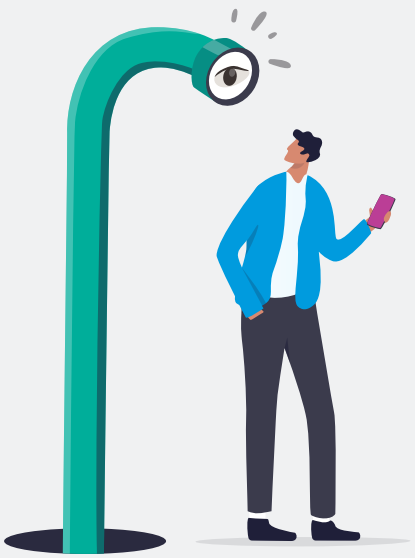
Una vez que consiguen acceder al sistema de un usuario con malware, credenciales robadas o una aplicación OAuth, los ciberdelincuentes pueden amenazar a sus empleados, sus datos y sus sistemas.

Así que, no es de extrañar que el tema de la seguridad ocupe ahora un lugar destacado en la agenda de la junta directiva. Por eso, proteger el entorno de Microsoft 365 es una decisión fundamental para la empresa. Todo programa de ciberseguridad eficaz pasa por dar prioridad a las personas.

No se puede proteger lo que no se ve

Proteger su despliegue de Microsoft 365, ya sea frente a las amenazas externas o las pérdidas de datos provocadas por los empleados, tiene un denominador común: la visibilidad.

Para descubrir y responder a los ataques de manera eficaz, necesita contar con la información adecuada. A menos que tenga una protección que le proporcione información amplia y detallada, será como encontrar una aguja en un pajar.



Bloquear las amenazas antes de que lleguen a la bandeja de entrada del usuario presenta dos ventajas fundamentales. En primer lugar, obtiene información sobre el ataque completo, no solamente de las últimas fases, una vez que el daño ya está hecho. En segundo lugar, al detectar las amenazas pronto, en el mejor de los casos antes de que lleguen a sus empleados, puede detenerlas antes de que pongan en riesgo su entorno.

Del mismo modo, no es posible proteger los datos ni responder a los incidentes de pérdida de datos sin una visibilidad que aproveche las características de Microsoft Information Protection (MIP). Necesita saber dónde residen sus datos sensibles y qué hacen sus usuarios con ellos. También necesita contexto para averiguar si un riesgo interno se debe a un usuario descuidado, malicioso o cuya cuenta ha sido comprometida.

Esto es aún más importante en un entorno empresarial tan cambiante como el actual. Los datos evolucionan con la misma rapidez que las innovaciones o adquisiciones. Para protegerlos, hacen falta funciones predictivas que indiquen qué datos son sensibles y así rodearlos de defensas que aprovechen mejor su inversión en MIP.

La combinación de seguridad aislada, DLP y cumplimiento de normativas no es viable

En el panorama de las amenazas actuales, que evoluciona continuamente, los ciberdelincuentes coordinan los ataques en varios vectores. A menudo, comprometen cuentas de usuario para tener acceso de nivel interno a datos, sistemas y otros recursos de valor.

Por eso, es vital contar con una defensa integrada y multicapa. Una solución eficaz debe integrarse con el resto del ecosistema de seguridad, protección de la información y cumplimiento normativo. Ahí se incluye todo, desde las defensas del correo electrónico hasta el sistema de prevención de la pérdida de datos (DLP), el agente de seguridad de acceso a la nube (CASB) y la plataforma de administración de identidades.

Una coordinación inteligente y automatizada ayuda a prevenir, detectar y responder a las amenazas que afectan a las personas a través de Microsoft 365.

Amenazas

La migración de los usuarios a OneDrive, Teams y otras aplicaciones de productividad de Microsoft 365 complica la seguridad de los datos. Necesita contar con capacidad para identificar y defender los datos que sus empleados crean, a los que acceden y que comparten.

Y con Microsoft 365 solamente esto no siempre es fácil. Es posible que la detección de amenazas nativa de la plataforma no proporcione la visibilidad que necesita de las ciberamenazas, la actividad de los usuarios y el desplazamiento de los datos en el correo electrónico, la nube y los endpoints.

Pérdida de datos

Todos los usuarios implican un cierto nivel de riesgo para sus empresas. Sin embargo, este riesgo es diferente para cada uno y cambia constantemente. Algunos usuarios actúan con motivaciones maliciosas, muchos son negligentes, y puede que otros tengan sus cuentas comprometidas. Por eso los modelos de seguridad universales y las políticas generales de acceso a los datos no protegen frente a los riesgos internos ni las amenazas dirigidas a personas a través de Microsoft 365.

Necesita visibilidad y controles que tengan en cuenta a las personas, los datos y las amenazas para obtener contexto en tiempo real. Solo entonces podrá evitar la pérdida y el uso ilícito de los datos en la organización.

Las interrupciones imprevistas del servicio de correo electrónico pueden tener un enorme impacto en la empresa

Las empresas actuales necesitan utilizar con confianza el correo electrónico. Una interrupción de su funcionamiento puede acarrear un alto coste. Por eso es fundamental garantizar el acceso ininterrumpido al correo electrónico.

Las interrupciones de servicio de Microsoft 365 están a la orden del día, pero no deberían paralizar sus operaciones. Busque funciones de continuidad de la actividad empresarial que aseguren la productividad de sus usuarios aun cuando Microsoft 365 esté fuera de servicio.

SECCIÓN 3

Cálculo del valor de una seguridad reforzada

Sobre el papel, prescindir de una solución de seguridad específica para su despliegue de Microsoft 365 puede parecer un ahorro,

pero la falta de una protección completa para su inversión probablemente acabará costándole tiempo, datos, dinero e incluso su reputación. A continuación describimos cómo aumentar las funciones nativas de Microsoft 365 puede ayudarle a garantizar su seguridad y el cumplimiento de las normativas.

Para los equipos de seguridad

La seguridad ha sido siempre una tarea difícil, y las amenazas avanzadas actuales la complican aún más. Ante las nuevas normativas y los ataques de gran envergadura, el tema de la seguridad llega hasta los consejos de administración, que ya no solo se preocupan de la eficacia, sino que valoran también tener visibilidad para saber qué amenazas se dirigen contra sus empleados y el riesgo inherente que suponen para la organización.

Amenazas

Carecer de la visibilidad y la información que necesita para afrontar los problemas de seguridad puede traducirse en una pérdida de tiempo. Según el Ponemon Institute, la detección y la respuesta sumaron la mayor parte de los costes de los incidentes de seguridad y llegaron a alcanzar 1,44 millones de dólares por incidente[8]. Se trata de una subida del 16 % respecto del año anterior y la primera vez en seis años que estos costes superan las pérdidas de negocio debidas a fugas de datos.

Los atacantes se sirven de las herramientas que utilizan los usuarios para hacer su trabajo. Ya se trate del secuestro de archivos fundamentales de SharePoint, el alojamiento de archivos maliciosos en OneDrive o el aprovechamiento de vulnerabilidades de Teams, los usuarios de Microsoft 365 se enfrentan a un aluvión de amenazas, por lo que precisan capas de seguridad adicionales.

Tenga en cuenta lo siguiente:

- ¿Cuánta productividad se pierde ocupándose de incidentes relacionados con el correo electrónico que podrían haberse prevenido?
- ¿Cuánto tiempo se emplea en identificar y corregir las cuentas comprometidas? ¿Cuánto en investigar, priorizar y confirmar las amenazas? ¿Y en eliminar los mensajes de correo electrónico que contienen adjuntos o URL maliciosos de los buzones de correo de sus usuarios?
- ¿Cómo cuantifica el riesgo de exposición prolongada de los usuarios a este tipo de mensajes?
- ¿Cuánto tiempo se pierde por una respuesta de seguridad descoordinada que no logra contener rápidamente las amenazas y proteger la reputación de su organización? (Puede ir de horas a días por alerta).
- ¿Cuánto tiempo extra añade una visibilidad limitada a sus esfuerzos para intentar conocer las amenazas que afectan a su entorno?
- ¿Cómo afecta a la seguridad que los usuarios recurran al correo personal durante una interrupción del servicio de Microsoft 365? (Un estudio de Gartner cifró una vez el coste en más de 300 000 dólares por hora[9]. Algunas interrupciones de servicio de Microsoft han durado días[10]).
- ¿Cuánto dinero está dispuesto a pagar para recuperar archivos secuestrados en ataques no detectados por Microsoft 365? (¿Y cuánto puede dedicar a restablecer las operaciones si no paga?)

8 Ponemon Institute. "Cost of a Data Breach Report 2022" (Informe sobre el coste de una fuga de datos en 2022), julio de 2022.

9 Andrew Lerner (Gartner). "The Cost of Downtime" (El coste de las interrupciones de servicio), julio de 2014.

10 Ed Targett (Computer Business Review). "Microsoft Office 365 Outage: Day Two as Enterprise User Grumbles Grow" (Interrupción de Microsoft Office 365: al segundo día aumentan las quejas de los usuarios de la empresa), enero de 2019.

Prevención de la pérdida de datos y protección de la información

Las empresas corren permanentemente el riesgo de sufrir una pérdida de datos. Puede ocurrir que los filtre algún empleado malintencionado o que los roben personas externas a la empresa, e incluso que empleados bienintencionados expongan activos que son vitales para la empresa de forma inadvertida.

Solo en 2021, las organizaciones denunciaron 1882 ataques contra los datos, un aumento del 68 % con respecto a 2020[11]. (Esta cifra incluye fugas, exposiciones y filtraciones).

La preocupación por la responsabilidad legal derivada de las fugas de datos ha alcanzado a los directivos de la empresa. A la vista de estos datos, debe ser crítico con la seguridad de Microsoft 365.

Revise la capacidad que ofrece para localizar datos confidenciales (de varios tipos de archivos), resolver problemas en todos los canales, e implementar y comunicar los problemas de las políticas. Plantéese reforzar las funciones nativas con una solución capaz de aplicar políticas al correo saliente, a OneDrive, SharePoint y Teams, así como ofrecer visibilidad del correo electrónico, los endpoints y la nube.

Los ataques contra los datos pueden proceder de usuarios maliciosos, negligentes o con cuentas comprometidas. Por lo tanto, no hay una única estrategia para resolverlos. Para saber a qué tipo de usuario se enfrenta, es fundamental contar con contexto e información.

Algunos factores que debe tener en cuenta son:

- ¿Cuál es el valor de los datos de Microsoft 365 que se llevan los empleados que dejan la empresa?
- ¿Cuánto costarían los datos robados o expuestos si la solución de DLP no puede proteger sus activos más valiosos en los principales canales en los que trabajan los empleados? ¿Es capaz de detectar datos confidenciales en todos los tipos de archivos que pueden contener información privada, en el correo electrónico, la nube y los endpoints?
- ¿Dispone de una vía centralizada para definir las políticas?
- ¿Puede descubrir rápidamente qué contenido y qué acciones han activado una alerta de infracción de una política? ¿Tiene el contexto que necesita para averiguar si un incidente interno ha sido provocado por un usuario malicioso, negligente o comprometido, y organizar la respuesta adecuada?
- ¿Está seguro de tener completamente protegida su propiedad intelectual?
- ¿Dispone de un flujo de trabajo de respuesta a incidentes para corregir los problemas? ¿Permite su respuesta automática efectuar simultáneamente bloqueos o correcciones en el correo electrónico, los recursos compartidos, Teams y los sitios de Microsoft SharePoint? ¿Necesita una solución DLP independiente para reducir la superficie de ataque en cada uno de estos canales? ¿Cómo mantiene estas políticas sincronizadas y la coherencia en los informes?
- Cuando investiga una alerta de DLP, ¿obtiene una visión significativa y fácil de entender de lo que ha ocurrido? ¿Es fácil compartirla con los equipos no técnicos del departamento jurídico y RR. HH.?
- ¿Puede ver quién ha accedido a datos y sistemas con privilegios y crear políticas para determinados individuos y grupos de personas?
- ¿Puede identificar rápidamente a qué aplicaciones de terceros de riesgo acceden sus empleados y proteger así a su empresa frente a ellas?

11 Identity Theft Resource Center. "First Half 2022 Data Breach Analysis" (Análisis de fugas de datos de la primera mitad de 2022), julio de 2022.

- Aparte de utilizar detectores integrados o personalizados para identificar datos sensibles, ¿puede aprender a descubrir riesgos de forma dinámica a partir de los datos mediante la inteligencia artificial y el aprendizaje automático?
- ¿Puede optimizar las políticas de DLP para mejorar su fiabilidad?

Para los departamentos de TI

Si es un administrador de TI, piense en el coste de las interrupciones y el soporte.

Tiempo de servicio y disponibilidad

Aunque Microsoft 365 promete un tiempo de funcionamiento continuo del 99,99 %, la realidad es un poco distinta. (Basta echar un vistazo al propio hilo de estado de Microsoft en Twitter para ver lo habituales que son los problemas de interrupciones de servicio).

Si tiene intención de incrementar la seguridad de Microsoft 365 y minimizar estos costes, hágase las siguientes preguntas:

- ¿Qué dependencia tiene su empresa del correo electrónico? ¿Cuáles serían las consecuencias de la pérdida de mensajes de clientes o clientes potenciales debido a una interrupción de la aplicación de correo electrónico?
- ¿Con qué frecuencia se interrumpe el flujo de correo electrónico de Microsoft 365?
- ¿Con qué rapidez se alerta al equipo de TI de una interrupción del servicio?
- ¿Dispone de suficientes datos y visibilidad para prever cuándo se restaurará el servicio?
- ¿Qué riesgos para la seguridad y el cumplimiento de normativas surgen cuando usuarios bienintencionados recurren a su correo electrónico personal para poder trabajar?

Seguimiento de mensajes, informe de mensaje no entregado (NDR)

Una pregunta que suelen recibir a diario los profesionales de seguridad y de TI es "¿Qué le ha ocurrido a mi correo electrónico?".

Analice su sistema detalladamente y conteste a las siguientes preguntas:

- ¿Cuánto tiempo puede dedicar a resolver estos problemas?
- ¿Con qué frecuencia se indexan los registros de mensajes? ¿Durante cuánto tiempo se conservan los registros?
- ¿Se tardan minutos u horas en obtener los resultados de la consulta?
- ¿Ha cambiado la experiencia de búsqueda en registros nuevos con respecto a la de los antiguos?
- ¿Dispone de los criterios de búsqueda necesarios para localizar registros rápidamente? ¿Son suficientes los detalles que se obtienen de las búsquedas?
- ¿Cuál es el proceso para contactar con el servicio de soporte en caso de que necesite información más detallada?
- ¿Cuál es el impacto de los falsos positivos en el volumen de seguimientos y el tiempo que se necesita?

Tiempo dedicado a la limpieza del correo electrónico y las máquinas

El equipo de TI puede dedicar horas, e incluso días, a restablecer la imagen inicial de las máquinas infectadas cuando los sistemas se ven comprometidos.

Además, debe eliminar estos mensajes para evitar la reinfección, que se produce cuando un usuario vuelve a acceder de manera inadvertida al contenido o incluso se lo reenvía a otro usuario.

Este proceso afecta a la productividad tanto del equipo de TI como de los usuarios, que pierden normalmente un día por incidente. Pregúntese lo siguiente:

- ¿En cuántas máquinas se debe restablecer la imagen inicial cuando esto podría ser innecesario o evitable?
- ¿Cuenta el equipo de TI con las herramientas necesarias para confirmar las infecciones y priorizar las máquinas que estaban expuestas, pero no se han visto afectadas?
- ¿Cuánto tiempo dedica el equipo de TI a la limpieza de mensajes?

Para el personal encargado del cumplimiento de normativas

El cumplimiento normativo hay que tomárselos en serio. Las consecuencias del incumplimiento pueden ser costosas y perjudicar seriamente a su empresa. A nivel de centro de datos, Microsoft 365 cumple las normativas principales. Entre ellas se encuentran el Reglamento general de protección de datos de la Unión Europea (RGPD), y la ley Health Insurance Portability and Accountability Act (HIPAA) o la ISO 27001, entre otras.

Sin embargo, la plataforma se ve limitada en lo que se refiere a archivado y supervisión de datos del correo electrónico, así como en cuanto a su disponibilidad en caso de litigio judicial o auditoría. No disponer de mecanismos de conservación de registros y flujos de datos que faciliten una defensa legal puede costar tiempo y recursos, e incluso conllevar gastos derivados de procedimientos acusatorios.

Probablemente necesite un plan de Microsoft 365 que incluya funciones para garantizar el cumplimiento de normativas o bien comprarlas como suscripción complementaria para garantizar la conformidad con las normativas de:

- Financial Industry Regulatory Authority (FINRA), Estados Unidos
- Securities and Exchange Commission (SEC), Estados Unidos
- Investment Industry Regulatory Organization in Canada (IIROC), Canadá
- U.K. Financial Services Act, Reino Unido

El objetivo de estas normas es proteger a los inversores, garantizando que los sectores de la seguridad en Estados Unidos, Reino Unido y Canadá funcionen con justicia y honestidad. Las multas por incumplimiento pueden alcanzar millones de dólares. Además, otros costes incluyen el del despliegue de medidas de seguridad adicionales, auditorías y posibles daños a la reputación.

Al evaluar las funciones predeterminadas de Microsoft 365, hágase estas preguntas importantes:

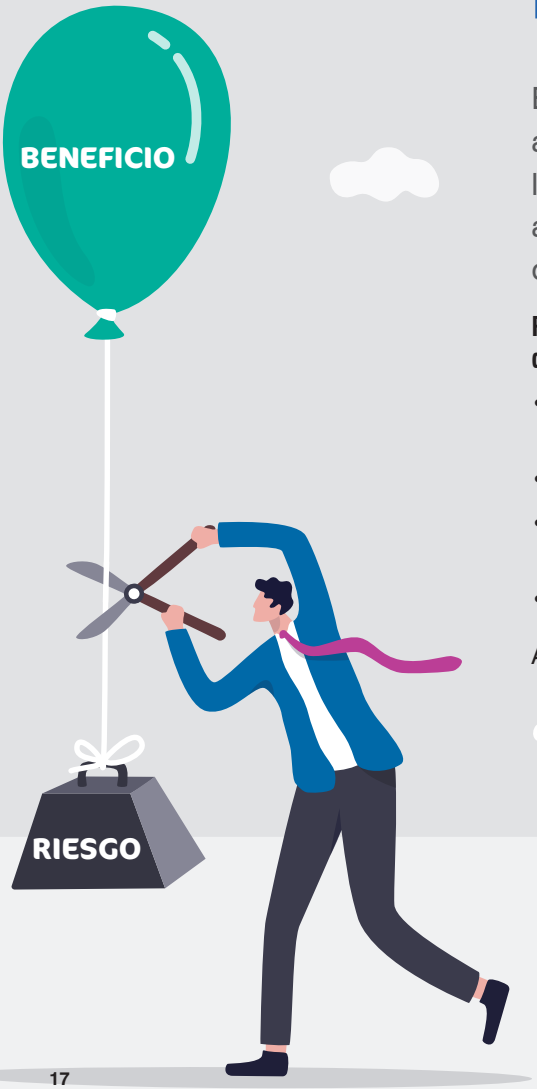
- En caso de que su empresa deba enfrentarse a una demanda judicial, ¿le permitiría Microsoft 365 proporcionar registros de todas las comunicaciones y transacciones de usuarios concretos, incluidas las de redes sociales y plataformas de colaboración empresarial? ¿Qué ocurre si tiene varios procesos en curso?
- ¿Hasta qué punto está en disposición de poner el contenido en suspenso por causas legales cuando surge un litigio jurídico?
- ¿Cuánto tiempo le lleva al equipo de TI realizar un descubrimiento electrónico, o eDiscovery, y exportar los datos? ¿Con qué rapidez se realizan las búsquedas? ¿Ofrece Microsoft un acuerdo de nivel de servicio (SLA) que defina los parámetros de esta función, que es fundamental? ¿Dónde se lleva a cabo el procesamiento de la búsqueda?
- Una vez que determina el conjunto de datos que desea exportar, ¿puede cargar los archivos en un sitio FTP específico de manera automática? ¿O bien debe reservar tiempo para realizar esta parte del flujo de trabajo de forma manual? ¿Cuáles son las consecuencias del retraso en la obtención de datos para el equipo de revisión?
- ¿Puede obtener y conservar todo el contenido de cumplimiento de normativas que genera su empresa? ¿Y los datos de las plataformas de medios sociales?
- ¿Hasta qué punto puede supervisar el contenido de manera satisfactoria? (Algunas normativas exigen que se supervise y se realice un muestreo del contenido). ¿Emplea tecnología punta o aplica una comparación básica de palabras clave?

12 Andrew Peck, Jennifer Feldman, *et al*. (New York Law Journal). "Defensible deletion: The proof is in the planning" (Eliminación defendible: la prueba está en la planificación), enero de 2021.

13 Chris Matthews (MarketWatch). "SEC fines JPMorgan $125 million for failing to keep records" (La SEC multa a JPMorgan con 125 millones de dólares por no guardar registros), diciembre de 2021.

SECCIÓN 4

Reducción del riesgo, simplificación de las operaciones y disminución del coste: la diferencia de Proofpoint



El panorama de las amenazas y el marco normativo en la actualidad, muy complejos y en continua evolución, exigen la aplicación de un nuevo enfoque a la protección frente a amenazas, la prevención de la pérdida de datos y el cumplimiento de normativas.

Por eso nosotros ofrecemos un enfoque exclusivo centrado en las personas que le proporciona:

- La protección frente a amenazas y la prevención de la pérdida de datos más eficaces del sector
- Visibilidad y contexto prácticos de las amenazas internas y externas
- Un enfoque moderno e integrado de los retos de las amenazas, la pérdida de datos y el cumplimiento de las normativas
- Una excelente experiencia para el usuario

Así puede mejorar la seguridad de Microsoft 365.

Protección reforzada frente al phishing, las estafas BEC y otras amenazas

Nuestro motor de detección basado en inteligencia artificial utiliza un análisis de comportamientos avanzado para detener una amplia variedad de amenazas, incluidas las que son difíciles de detectar porque no utilizan URL ni adjuntos maliciosos, como los ataques BEC.

Mediante el uso del aprendizaje automático y el análisis de comportamientos, entrenados con billones de puntos de datos, detectamos y bloqueamos al mes 2,2 millones de amenazas BEC. Facilitamos análisis forenses detallados para que entienda por qué se ha identificado como BEC y se ha bloqueado un mensaje.

También consigue saber:

- A quién van dirigidas las estafas BEC en la empresa
- Los principales temas de los ataques BEC dirigidos a su organización
- La tendencia en el tiempo de las amenazas BEC en su organización

Nuestra solución integrada y holística proporciona amplia visibilidad de las actividades y los comportamientos maliciosos de los usuarios para detener otras amenazas modernas. Además, automatiza los principales elementos del proceso de respuesta a incidentes para que pueda proteger a los usuarios a gran escala.

El análisis predictivo de URL identifica y neutraliza las direcciones URL no seguras antes de que se entreguen y cuando los usuarios hacen clic. Puede bloquear los adjuntos que contengan URL no seguras y reescribir las URL sospechosas independientemente de que aparezcan en archivos de texto (.txt), archivos de texto enriquecido (.rtf) o HTML.

Con un tiempo de análisis medio de menos de tres minutos, bloqueamos los adjuntos no seguros antes de que los usuarios tengan la oportunidad de interactuar con ellos, y sin reducir la productividad. Admitimos una amplia variedad de tipos de archivos, incluidos PDF y HTML, no solo los archivos de Office.

Con los usuarios y sitios web de alto riesgo, nuestra tecnología de aislamiento de URL abre enlaces desconocidos de correo electrónico en un espacio seguro y autónomo para mantener las amenazas fuera de su entorno.

Y las etiquetas de advertencia de correo electrónico configurables, junto con las denuncias con un solo clic, alertan a los usuarios para que adopten precauciones adicionales y facilitan la denuncia de mensajes potencialmente maliciosos.

La seguridad de los datos más eficaz del sector

Proteja los datos frente a las amenazas externas e internas con un contexto centrado en las personas que correlaciona el contenido, los comportamientos y las amenazas. Nuestra vista cronológica reconstruye qué ha ocurrido con cada alerta de DLP. Puede evaluar rápidamente las intenciones de los usuarios, colaborar fácilmente con otros equipos, como el departamento jurídico y de RR. HH., y adoptar las medidas adecuadas.

Facilitamos la creación, aplicación y ejecución de políticas unificadas para el correo electrónico, la nube y los endpoints que le permitan proteger sus datos y garantizar el cumplimiento de las normativas.

Nuestro motor de clasificación de datos basado en inteligencia artificial activa inmediatamente el programa de DLP y optimiza su flujo de trabajo. Puede elegir entre cientos de clasificadores entrenados previamente o dejar que nuestro motor de DLP cree clasificadores personalizados a partir de los documentos que se le indiquen. El motor aprende dinámicamente a partir de los datos almacenados en repositorios locales y cloud para proponer diccionarios que pueden aplicarse en todos los canales con un solo clic.

El análisis algorítmico, nuestro motor de identificadores inteligentes y los diccionarios incorporados le permiten centrarse en la definición y el mantenimiento de las políticas de datos específicas de su organización. Nuestros flujos de trabajo de DLP instantáneos también facilitan la búsqueda, gestión y denuncia de las violaciones de datos.

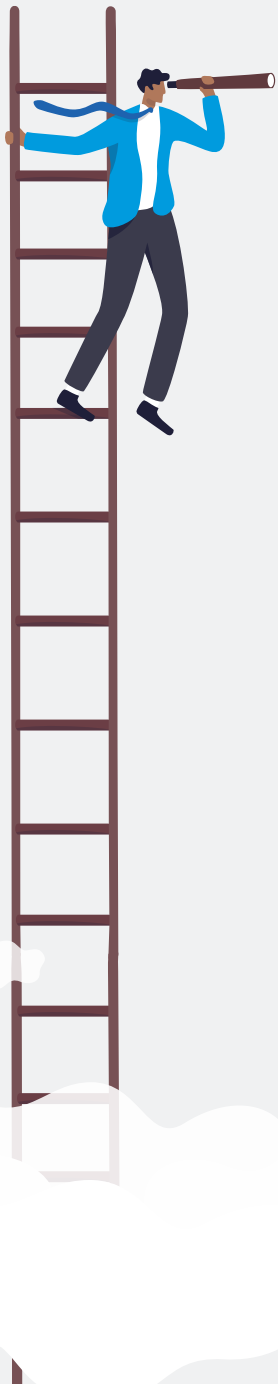
Protección frente a la usurpación de cuentas

Gracias a nuestro enfoque multicapa, le ayudamos a proteger su cuenta de Microsoft 365 con alertas de actividad sospechosa en tiempo real, corrección automatizada y controles de acceso basados en los riesgos.

Cuando se producen los incidentes, nuestro intuitivo panel le permite investigar la actividad anterior y las alertas. Nuestras eficaces políticas le alertan de los problemas en tiempo real, corrigen las cuentas comprometidas, ponen en cuarentena los archivos maliciosos y aplican autenticación basada en el riesgo cuando es necesario.

La integración con Okta ayuda a identificar varias actividades anómalas o no seguras, como:

- Inicios de sesión en Microsoft 365 correctos pero sospechosos
- Inicios de sesión fallidos
- Acceso imprevisto a aplicaciones empresariales
- Escalamientos de privilegios que permiten acceder a recursos cloud de valor
- Escalamientos que eximen al usuario de los factores de autenticación habituales



Mayor visibilidad y seguridad en la nube

Adoptamos un enfoque centrado en las personas para proteger frente a amenazas de la nube, descubrir las shadow IT y gestionar las aplicaciones cloud y OAuth de terceros.

Vamos mucho más allá de la seguridad nativa de Microsoft 365 para proteger a los usuarios, los datos sensibles y las apps cloud frente a amenazas internas y riesgos de incumplimiento. Identifique a sus VAP (Very Attacked People™ o personas muy atacadas) y aplique controles basados en riesgos para mantener protegidas sus cuentas.

Respuesta a incidentes ultrarrápida a escala

Elimine automáticamente el correo electrónico malicioso de la bandeja de entrada, incluidos los mensajes denunciados por los usuarios o calificados de inseguros una vez entregados. Cuando se detectan mensajes maliciosos, los eliminamos automáticamente de la bandeja de entrada de los usuarios, incluso si se han reenviado a otras personas. Esta función reduce enormemente el tiempo que dedican los equipos de seguridad y mensajería a investigar y resolver las amenazas del correo electrónico.

También corregimos las usurpaciones de cuentas antes de que provoquen daños duraderos a sus datos, sus operaciones, las relaciones de su empresa y su reputación.

Archivado inteligente a toda velocidad

Con independencia del tamaño que alcance su archivo, garantizamos que sus búsquedas tardarán como máximo 20 segundos, en lugar de minutos u horas.

Nuestro archivado cloud admite más de 500 tipos de archivos en la nube o de forma local, no solo el correo electrónico. Y no limitamos el número de casos eDiscovery (descubrimiento electrónico), retenciones por causas legales y exportaciones de datos que puede incluir, ya sean 10 000 buzones de correo o 100 000 (o más).

Programas para concienciar en seguridad que modifican el comportamiento de los usuarios

Ofrecemos una inmensa biblioteca de atractivo contenido basado en las técnicas de atacantes del mundo real. Incluye nuestra propia inteligencia sobre amenazas y las lagunas de conocimiento únicas de sus usuarios. Y es lo suficientemente flexible para personalizarla en función de los retos de seguridad exclusivos de su organización y encajar en el horario de los usuarios.

Además de formación de concienciación básica, ofrecemos simulaciones de phishing y formación complementaria puntual para los usuarios que "muerden el anzuelo". Facilitamos el seguimiento y comunicación del progreso a lo largo del tiempo para que pueda identificar áreas de mejora y ayudar a los usuarios a progresar.

Soporte de talla mundial

Instalamos y personalizamos completamente su despliegue en función de las últimas tendencias y las mejores prácticas del sector. Después del despliegue, ofrecemos soporte permanente durante todo el año, sin complicados complementos de servicio.

Tenemos una tasa de satisfacción del cliente continua de más del 95 % y una tasa de renovación anual de más del 90 %. No es de extrañar que entre nuestros clientes se incluyan más de la mitad de las empresas Fortune 100.

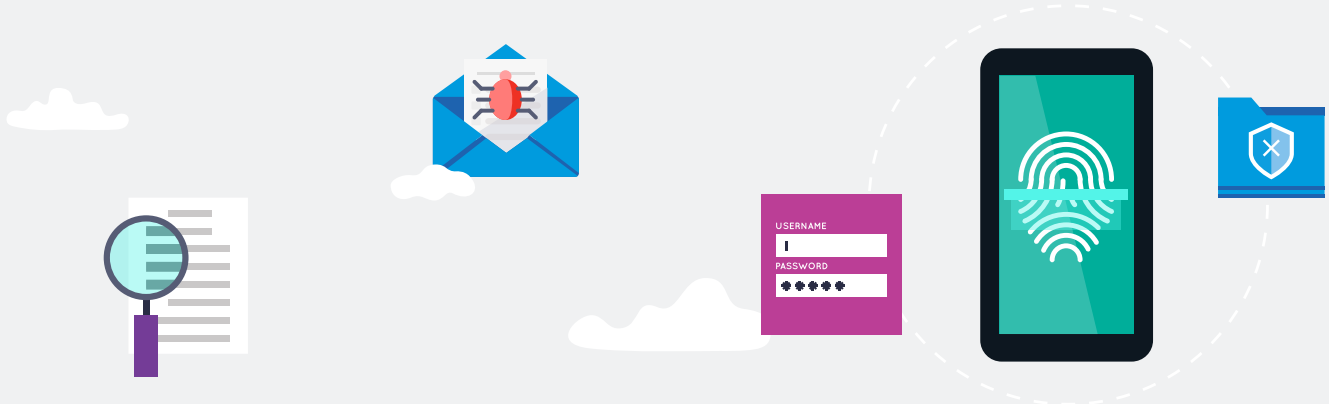
Seguridad completa y totalmente integrada que optimiza las operaciones

Nuestra plataforma de seguridad completa e integrada combina una protección potente y eficaz del correo electrónico, la nube y la información para hacer frente a los mayores retos de seguridad y cumplimiento de la actualidad. También ofrecemos integración con los mejores proveedores de seguridad, como Palo Alto Networks, Okta y CrowdStrike, para optimizar su flujo de trabajo y ayudar a su equipo de seguridad a trabajar mejor y más rápidamente.

Todo se suma para proporcionarle una seguridad unificada, centrada en las personas, que proteja su entorno de Microsoft 365.

Nuestro enfoque de seguridad y cumplimiento de normativas para Microsoft 365:

- Reduce sus riesgos
- Libera importantes recursos de seguridad y TI
- Recorta costes
- Refuerza la eficacia de sus operaciones de seguridad



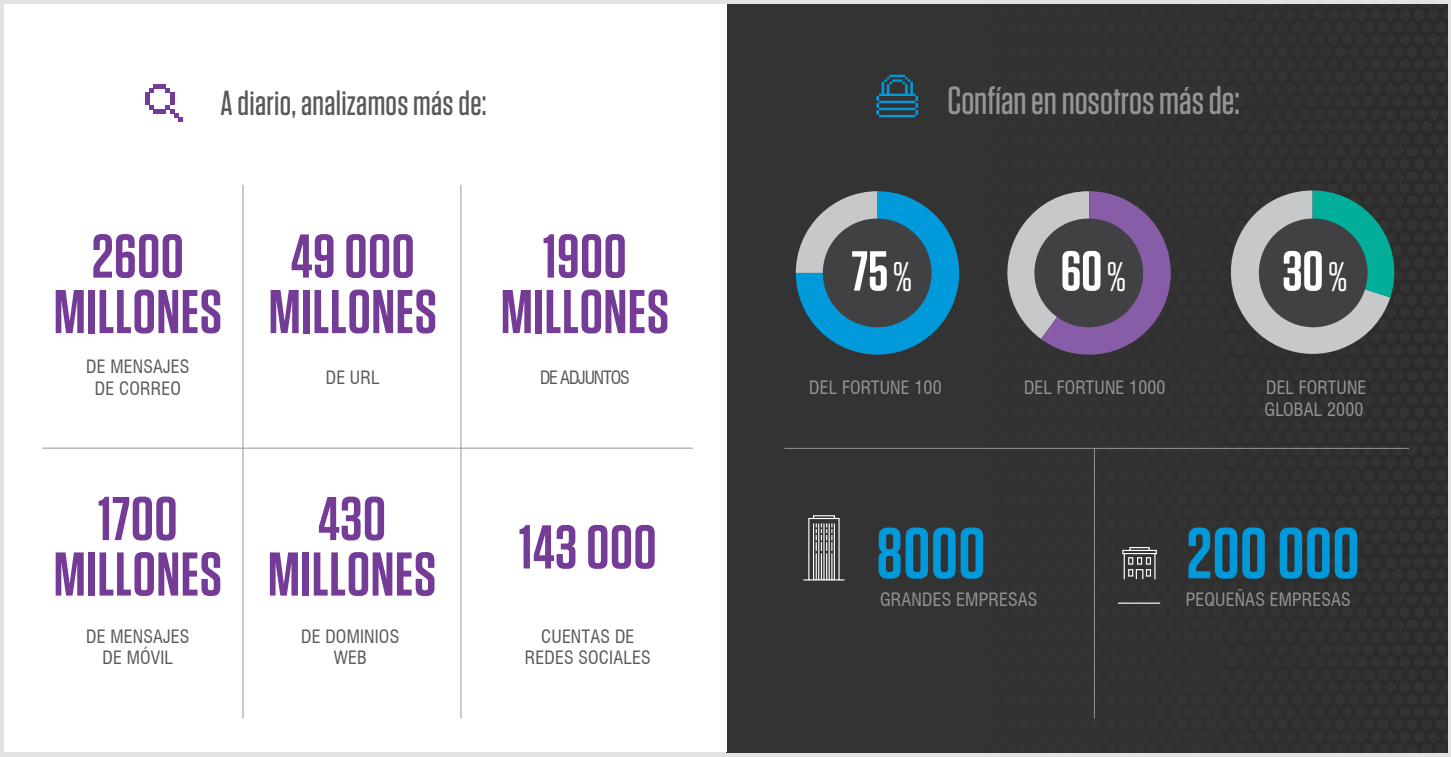
SECCIÓN 5

Dé los pasos siguientes

Infórmese sobre Proofpoint y sobre cómo podemos ayudarle a ampliar su despliegue de Microsoft 365 con protección centrada en las personas, prevención de la pérdida de datos y cumplimiento de normativas para el correo electrónico, la nube y los endpoints en proofpoint.com.

Acerca de Proofpoint

El gráfico de amenazas Nexus de Proofpoint combina lo mejor en investigación de seguridad, tecnología y datos de amenazas para mantenerle siempre protegido en todas las fases del ciclo de vida de los ataques. Nadie conoce mejor los ciberataques actuales, cuyo objetivo son las personas.



MÁS INFORMACIÓN

Para obtener más información, visite **proofpoint.com/es**.

ACERCA DE PROOFPOINT

Proofpoint, Inc. es una compañía líder en ciberseguridad y cumplimiento de normativas que protege el activo más importante y de mayor riesgo para las organizaciones: las personas. Gracias a una suite integrada de soluciones basadas en cloud, Proofpoint ayuda a empresas de todo el mundo a detener las amenazas dirigidas, a salvaguardar sus datos y a hacer a los usuarios más resilientes frente a ciberataques. Compañías líderes de todos los tamaños, entre las que se encuentra el 75 % del Fortune 100, confían en las soluciones de Proofpoint para su seguridad centrada en personas y su cumplimiento regulatorio, mitigando los riesgos más críticos en sus sistemas de correo electrónico, cloud, redes sociales y web. Encontrará más información en **www.proofpoint.com/es**.

proofpoint.

0501-004-06-02 10/22